ITS Mississippi Department of Information Technology Services

Enterprise Security Policy

Version 1.0: 3/26/07

Enterprise Security Policy

Table of Contents

I. Introduction

The purpose of the Information Technology (IT) Security Policy is to create an environment within state of Mississippi agencies that maintains system security, data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data. It is the intent of the Mississippi Department of Information Technology Services (ITS) that state agencies will adhere to the policies identified in this document and use the guidelines as a standard in which to develop, implement, and maintain security plans pertinent to their specific technology areas. Each agency is responsible and accountable for its own security plan and should educate employees to follow security procedures. Technological advances and changes in the business requirements will necessitate periodic revisions; therefore, agencies should review and update IT security plans at least annually or following any significant change to its business, computing, or telecommunications environment.

II. Purpose of Security Policy

The state's transition from multiple proprietary network connections over dedicated leased networks to the Internet for conducting vital public business has highlighted the following security concerns:

- Information Integrity - Unauthorized deletion, modification or disclosure of information;
- Misuse - The use of information assets for other than authorized purposes by either internal or external users;
- Information Browsing - Unauthorized viewing of sensitive information by intruders or legitimate users;
- Penetration - Attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs;
- Computer Viruses – Attacks using viral code that reproduces itself by modifying other programs, spreading across multiple programs, data files or devices on a system or through multiple systems in a network, that may result in the destruction of data or the erosion of system performance;
- Fraud - Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in financial loss or embarrassment to the organization;
- Component Failure - Failure due to design flaws or hardware/software faults can lead to denial of service or security compromises through the malfunction of a system component; and
- Unauthorized additions and/or changes to infrastructure components.

Because information technology security planning is primarily a risk management issue, this policy and its associated standards and guidelines focus on the creation of a shared and trusted environment, with particular attention to:

- Common approaches to end-user authentication;
- Consistent and adequate network, server, and data management;
- Appropriate uses of secure network connections; and
- Closing unauthorized pathways into the network and into the data pursuant to Mississippi Code Annotated, § 25-53-3.

Such an environment is made possible through an enterprise approach to security in state government that:

- Promotes an enterprise view among separate agencies;
- Requires adherence to a common security architecture and its related procedures;
- Recognizes an interdependent relationship among agencies, such that strengthening security for one strengthens all and, conversely, weakening one weakens all; and
- Assumes mutual distrust until proven friendly, including relationships within government, with trading partners, and with anonymous users.

In response to these threats and to assist state agencies in mitigating associated risks, ITS requires that agencies take steps necessary to initiate an enterprise-wide approach to:

- Ensure secure interactions between and among governmental agencies take place within a shared and trusted environment;
- Ensure secure interactions between and among business partners, external parties and state agencies utilize a common authentication process, security architecture, and point of entry;
- Prevent misuse of, damage to, or loss of IT hardware and software facilities;
- Ensure employee accountability for protection of IT assets; and
- Prevent unauthorized use or reproduction of copyrighted material by public entities.

Accordingly, ITS directs state agencies to:

- Operate in a manner consistent with the Information Technology (IT) Security Policy of the State of Mississippi;
- Develop, implement, maintain, and test security processes, procedures, and practices to protect and safeguard voice, video, and data computing and telecommunications facilities -- including telephones, hardware, software, and personnel -- against security breaches;

- Train staff to follow security procedures and standards;
- Apply appropriate security measures when developing transactional Internet-based applications, including but not limited to electronic commerce (e-commerce); and
- Ensure and oversee compliance with this policy.

III. Statutory Authority

The provisions of § 25-53-1 to § 25-53-25 of the Mississippi Code Annotated detail the powers and duties of the Mississippi Department of Information Technology Services (ITS), including the authority to develop statewide or interagency information services and technical policies, standards and procedures.

IV. Security Policy Scope

For the purposes of this policy, security is defined as the ability to protect the integrity, availability, and confidentiality of information held by an agency and to protect IT assets from unauthorized use or modification and from accidental or intentional damage or destruction. It includes the security of IT facilities and off-site data storage; computing, telecommunications, and applications related services purchased from other state agencies or commercial concerns; and Internet-related applications and connectivity.

This policy applies to all executive and judicial branch agencies and educational institutions, as provided by law, that operate, manage, or use IT services or equipment to support critical state business functions.

V. Security Policy Exemptions

This policy applies to Institutions of Higher Education except, pursuant to section § 25-53-25 of the Mississippi Code Annotated, when they develop security policies in lieu of the policy statements below that are:

1) Appropriate to their respective environments, and

2) Consistent with the intent of the ITS policy. Such higher education security policies must address:

- Appropriate levels of security and integrity for data exchange and business transactions;
- Effective authentication processes, security architecture(s), and trust fabric (s); and,
- Compliance, testing and audit provisions.

VI. General Security Policy

It is the IT security policy of the State of Mississippi that:

1) Each agency shall operate in a manner consistent with the maintenance of a shared, trusted environment within state government for the protection of sensitive data and business transactions. Agencies may establish certain autonomous applications, including those hosted by an Applications Service Provider or other third party, outside of the shared, trusted environment, **PROVIDED** the establishment and operation of such applications follows all guidelines as set forth in this security policy and does not jeopardize the enterprise security environment, specifically:

- The security protocols (including means of authentication and authorization) relied upon by others; and
- The integrity, reliability and predictability of the State backbone network.

2) Each agency shall establish its secure state business applications within the guidelines of the Mississippi State Government Network Infrastructure. This requires that all parties interact with agencies through a common security architecture and authentication process. ITS shall maintain and operate the shared infrastructure necessary to support applications and data within a trusted environment.

3) Furthermore, each agency that operates its applications and networks within the Mississippi State Government Network Infrastructure must subscribe to the following principles of shared security:

- Agencies shall follow security standards established for selecting appropriate assurance levels for specific application or data access and implement the protections and controls specified by the appropriate assurance levels;
- Agencies shall recognize and support the state's standard means of authenticating external parties needing access to sensitive information and applications;
- Agencies shall follow security standards established for securing servers and data associated with the secure application; and
- Agencies shall follow security standards established for creating secure sessions for application access.

4) Each agency must address the effect of using the Internet to conduct transactions for state business with other public entities, citizens, and businesses. Plans for Internet-based transactional applications, including but not limited to e-commerce, must be prepared and incorporated into the agency's portfolio and submitted for security validation.

5) Each agency must ensure staff is appropriately trained in IT security procedures. Each agency must make staff aware of the need for IT security and train them to perform the security procedures for which they are responsible. Agencies are encouraged to participate in appropriate security alert response organizations at the state and regional levels.

6) Each agency must review its IT security processes, procedures, and practices at least annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment. Examples of these changes include modifications to physical facility, computer hardware or software, telecommunications hardware or software, telecommunications networks, application systems, organization, or budget. Practices will include appropriate mechanisms for receiving, documenting, and responding to security issues identified by third parties.

7) Each agency must conduct an IT Security Policy and Standards Compliance Audit once every three years. The audit must be performed by knowledgeable parties independent of the agency's IT organization, such as the State Auditor. The work shall follow audit standards developed and published by the State Auditor. The State Auditor may determine an earlier audit of an agency's IT processing is warranted, in which case they will proceed under their existing authority. The nature and scope of the audit must be commensurate with the extent of the agency's dependence on secure IT to accomplish its critical business functions. Each agency must maintain documentation showing the results of its review or audit and the plan for correcting material deficiencies revealed by the review or audit. To the extent that the audit documentation includes valuable formulate, designs, drawings, computer source codes, object codes or research data, or that disclosure of the audit documentation would be contrary to the public interest and would irreparably damage vital government functions, such audit documentation is exempt from public disclosure.

8) Agency heads are responsible for the oversight of their respective agency's IT security and will confirm in writing that the agency is in compliance with this policy. The annual security verification letter must be included in the agency IT portfolio or submitted to the ITS. The verification indicates review and acceptance of agency security processes, procedures, and practices as well as updates to them since the last approval.

9) The State Auditor may audit agency IT security processes, procedures, and practices. The State Auditor may audit any agency pursuant to Mississippi Code Annotated (Supp. 2001), Section 7-7-211 for agency compliance with this policy. Agency IT security processes, procedures, and practices may contain information (confidential or private) about the agency's business, communications, and computing operations or employees. Policy and procedures for distribution of any related documentation should consider sensitive information and related statutory exemptions for such information from public disclosure.

10) ITS recommends that Agencies obtain security risk assessments from third-party security consultants from time to time. A security risk assessment is a valuable tool that helps IT management and system/network administrators identify their vulnerabilities so those vulnerabilities may be addressed. However, information contained within the resulting reports and/or documentation of an assessment could be a security risk if in the "wrong" hands. Please be advised that any reports and/or documents resulting from a security risk assessment are classified as confidential and are not to be made available for public disclosure in accordance with Section 25-61-9 of the Mississippi code annotated.

VII. Maintenance of Policies, Standards, Guidelines and Recommendations

Technological advances and changes in the business requirements of State agencies will necessitate periodic revisions to policies, standards, guidelines and recommendations. ITS is responsible for routine maintenance of these to keep them current. Major policy changes will require the approval of ITS.

VIII. Security Policy; Review, Schedule and Updates

Technological advances and changes in the business requirements will necessitate periodic revisions; therefore, agencies should review and update IT security plans at least annually or following any significant change to its business, computing, or telecommunications environment.

If an agency purchases IT services from another organization, the agency and the service provider should work together to make certain the IT security plan for the service provider fits within the agency's plan. If two or more agencies participate with each other in operating an information service facility then the agencies should develop a joint IT security plan which meets their mutual needs.

Agencies should promote security awareness by informing employees, associates, business partners, or others using its computers or networks about security policies and practices, what is expected of them, and how they are to handle the information.

IX. Security Officers; Role and Responsibilities

ITS will designate a Security Officer that is responsible for developing and maintaining the State of Mississippi Enterprise Security Policy. The ITS Security Officer will:

- Develop and maintain the State of Mississippi Enterprise Security Policy
- Research the IT industry for security related issues and determine how it effects the State IT infrastructure as a whole
- Participate in local and national security organizations for the purpose of sharing security information, pitfalls, warnings, etc.

- Work with State agencies on all related security issues
- Maintain a State Network Security Listserve for the purpose of distributing security advisories and facilitating security discussion among the State network participants
- Work with the State Network Operation Center in investigating intrusion attempts and virus attacks. Reporting to agencies' on these intrusion attempts and virus attacks.
- Work with State Auditor's Office on Security Audits as necessary

ITS requires that each agency designate an individual to serve as a contact for ITS concerning all security-related issues. In addition, ITS **highly** recommends that each agency designate an individual(s) as their agency's Security Officer. For agencies with small IT infrastructures, this designation could be a minor/shared duty assumed by an existing member of the agency staff. For other agencies with very large/complex IT infrastructures, this designation should require that security be a major duty for that individual or possibly multiple individuals. The agency Security Officer will:

- Develop and maintain Agency-specific security policies
- Be ITS's primary contact for security related issues
- Ensure that Agency is adhering to State of Mississippi Enterprise Security Policy
- Participate in the State Network Security Listserve
- Research IT industry for security related issues and how it effects their agency specifically
- Monitor security issues within the agency's IT resources.
- Facilitate the State Auditor's Office Security Audit

X. Auditing and Compliance; State Auditor's Role

Compliance with security policies is the responsibility of all state agencies. Any agency that fails to comply with security policies endangers everyone else in state government. Thus the following policy is established to clarify the role of the State Auditor and the Department of Information Technology Services in auditing compliance:

The State Auditor will assess how well agencies comply with security policies as part of normal agency auditing activities. The State Auditor may request the assistance of ITS in the performance of this function. Additionally, the State Auditor may be requested to perform a special audit of any agency's compliance with security policies if there is just cause for suspecting non-compliance.

Upon determination of any non-compliance, the State Auditor may instruct the agency and/or ITS to take necessary steps to become compliant.

XI. Web Server; Connectivity, Security, Physical Location

If an Agency maintains a web sever that resides on the State network and needs it to be mapped through the firewall so that it is accessible from the Internet, there are several security guidelines that must be met. These include:

1) ITS will perform network address translation (NAT) to convert the private IP address to a public IP address so the server may be accessible from the Internet. However, ITS will only open up ports HTTP and/or HTTPS for this sever.

2) Agency is required to "harden" the server by making sure that all the current operating system patches are applied and kept up-to-date, removing any unnecessary server processes, etc.

3) Physical Location: ITS will permit this web server to be physically located on the Agency local network. However, ITS recommends that the Agency consider placing that Internet-accessible web server on a "de-militarized zone" or DMZ segment behind a firewall. If the web server were hacked, the hacker would only then have access devices that reside within the DMZ and not the rest of the agency's local network and/or the rest of the State network. As an alternative, ITS recommends that the Agency consider physically locating the web server within the ITS DMZ located within the State Computer Center. Locating the web server in the ITS DMZ will ensure that if a hacker does break into the web server, they will not have access to the rest of the state network. Although the ITS DMZ is within a secure, restricted area, agencies' locating servers there will still have 24/7 access to their equipment.

XII. E-mail; Functionality, Security, Limitations

For the purpose of security and limiting spam into the network, ITS has implemented and maintains mail relays on the inside and outside of the firewall. All mail bound for State domain email addresses must come through the outside mail relay and be "relayed" to the inside mail relay. The inside mail relay forwards the mail on to the appropriate mail server. Also, all mail going out hits the inside mail relay first and then is "relayed" to the outside mail relay before being forwarded to the Internet. For this reason, agencies must adhere to the following guidelines in regard to incoming/outgoing mail:

1) No direct SMTP to and/or from the Internet. Agencies must utilize the ITS maintained mail relays for mail traveling in both directions.

2) No POP or IMAP from Internet to mail servers inside State network. Agencies must utilize a web interface (HTTP/HTTPS) to access this mail.

3) No POP or IMAP from State network to private mail accounts on Internet. Agencies must utilize a web interface (HTTP/HTTPS port) to access this mail.

4) The maximum file size for attachments is 10MB. Any emails with attachments larger than 10MB will be discarded. If there is a need to email a file larger than 10MB, the file should be compressed using an industry standard file compression utility (ie. WinZip, etc.).

ITS also recommends the following guidelines to provide agencies with an example of acceptable use for the sending and receiving of electronic mail. Electronic mail (email) is increasingly critical to the normal conduct of business. Email should be used with the same care and discretion as any other type of official agency communication. Policies should be established to help employees use email properly, to reduce the risk of intentional or inadvertent misuse, and to assure that official records transferred via electronic mail are properly handled. Principle priorities are:

1) Email communications should not be unethical, fraudulent, harassing, obscene, be perceived to be a conflict of interest, or contain sensitive/confidential information (i.e. credit card numbers, social security numbers, etc.)

2) File attachments sent via e-mail should be scanned using current anti-virus software prior to sending the transmission. Any file attachment that is received should be scanned prior to opening the file.

4) Users should not allow anyone else to send email using their accounts.

5) Email should be used to conduct official business only.

6) It is recommended that State agencies require a confidentiality statement at the end of each email transmitted from their agency. An example of one such statement is below:

"Confidentiality Note: The information contained in this e-mail and/or document(s) attached is for the exclusive use of the individual named above and may contain confidential, privileged and non-disclosable information. If you are not the intended recipient, you are hereby notified that you are strictly prohibited from reading, photocopying, distributing or otherwise using this e-mail or its contents in any way. If you have received this transmission in error, please notify me immediately."

XIII. Antivirus Software; Virus Prevention, Detection and Removal

There are several kinds of software that can surreptitiously breach computer and/or network security. They include:

Virus: a code fragment (not an independent program) that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources, which are then not available to authorized users.

Worm: an independent program that reproduces by copying itself from one system to another, usually over a network. Like a virus, a worm may damage data directly, or it may degrade system performance by consuming system resources and even shutting down a network.

Trojan horse: an independent program that appears to perform a useful function but that hides another unauthorized program inside it. When an authorized user performs the apparent function, the Trojan horse performs the unauthorized function as well (often usurping the privileges of the user).

A common method of sending these computer viruses is via email. ITS will scan all inbound email for viruses. ITS recommends that all Agencies implement administrative policies in regard to virus and email. These should include:

1) Maintain virus scanning software on the network including all servers and workstations.

2) Be diligent about keeping virus definition files up-to-date. The virus scanning software is only as good as the virus definition file associated with the scan. Virus scan performed with out-dated definitions file will not locate the newest, latest and greatest virus threat.

3) Instruct network users not to open attachments from individuals they do not know and/or trust. Instruct them to either delete the email in question or notify the support staff for further investigation.

4) Once a device is infected with a virus, the offending machine should be removed from the network until such time the virus can be removed from the machine. If ITS detects that a machine located on an Agency local network is infected with a virus, access will be blocked from the rest of the State network to/from that machine so the virus will not be spread to other machines on the State network. When the Agency notifies ITS that the virus has been removed, access will be restored.

5) Please note that copies of virus-detection and eradication tools should be kept offline. Otherwise it is possible that the virus could modify the detection tools to prevent its own detection. You should actively scan/check for viruses online, but periodically use the off-line, trusted copies of the tools to scan your systems.

XIV. Firewalls Requirements; Use, Functionality and Port Restriction

ITS will maintain a firewall within the core of the network that provides one level of protection of the State network from the connection to the Internet. However, Agencies are encouraged to implement firewalls on their networks that provide a second level of protection from the Internet, as well as, protect their network from the rest of the State network.

In the firewall that protects the State network from the Internet, only HTTP and HTTPS ports will be opened from the Internet to the state network. All other ports will be closed. Below are examples of what will not be permitted:

1) No direct SMTP to and/or from the Internet. Agencies must utilize the ITS maintained mail relays for mail traveling in both directions.

2) No POP or IMAP from Internet to mail servers inside State network. Agencies must utilize a web interface (HTTP/HTTPS) to access this mail.

3) No POP or IMAP from State network to private mail accounts on Internet. Agencies must utilize a web interface (HTTP/HTTPS port) to access this mail.

4) No FTP access allowed from Internet to a device on State network.

5) ITS will not restrict FTP out of the State network to a device on the Internet provided that session/transfer is initiated from the State network.

6) No LAN protocols mapped to and/or from devices on Internet (ie. NetBios, NetBeui, NFS, etc.).

7) No ICMP to and/or from Internet to State network.

8) Any outbound port that has the potential of propagating industry-known viruses, worms, etc.

The exception to these port restrictions is when an Agency has a VPN implemented between themselves and a third party. In that scenario, all ports are available for use provided the traffic goes through the VPN.

If the Agency has a web server that resides on the Agency local network and needs that web server to be mapped through the firewall for access by individuals in the Internet, then the agency should provide ITS the private IP address and the host name of the server. ITS will build a conduit in the firewall that performs network address translation and create a DNS entry for the server. It should be noted that only HTTP and HTTPS ports will be open through the conduit.

XV. Data Encryption; Requirements and Recommendations

ITS requires that all sensitive data be encrypted when traveling to/from untrusted networks and/or entities.

If an agency Internet-facing server gathers or transmits sensitive data (i.e. name, address, phone, credit card number, SSN, DLN) from customers, then the application must use, at minimum, SSL for the transaction. It is recommended that a reputable 3rd party server certificate be used for this SSL transaction. If agency security requirements for an application require client-based digital certificates, the agency must consult with ITS before implementation in the event a global solution is the best case scenario.

The encryption method for all virtual private networks must be either industry-standard IPSec or SSL protocols.

It is recommended Agencies consider the encryption of sensitive data at any point it leaves their local trusted network. For example, if Agency A must send sensitive data to Agency B, the sensitive data must leave Agency A's local trusted network and travel a common, shared (State) network infrastructure to get to Agency B's trusted local network. The encryption of this sensitive data could prohibit a hacker residing on the common, shared infrastructure from capturing this sensitive data as it travels from A to B.

It is also recommended that if the agency stores that sensitive information on a server, the sensitive data be encrypted.

XVI. Remote Network Access; Virtual Private Network Requirements

The following policies address connectivity into the State network from any entity that resides outside the trusted State network (ie. outside State border firewall). This includes third party entities' connectivity into the State network via the public Internet, as well as, private circuits.

1) All connections from any entities (State or third party) that reside on the outside of the trusted State network (ie. outside State border firewall) must be made via a virtual private network (VPN) using industry-standard IPSec or SSL protocols.

2) Split-tunneling MUST be disabled on any device (firewall, VPN Concentrator, etc.) used to terminate VPNs behind the State's firewall and/or the agency's firewall or any remote device/software that utilizes the VPN.

a. Split-tunneling renders the State's firewall and the agency's firewall useless by allowing information to be relayed as trusted traffic from the insecure Internet onto the State's Network. Split-tunneling directly violates the security policy by circumventing all security precautions that are taken to preserve the integrity of the State Network.

b. It should be understood that split tunneling is defined as having the ability to participate in a LAN while connected to the State Network via VPN. To meet the requirement of disabling split tunneling, it is required that all network activity for the client pc be redirected down the tunnel. Both listening services and browsing services must be redirected to the VPN so that no LAN activity can take place, regardless of whether it is initiated by the client pc or by another device on the LAN.

c. Any device (including SSL VPN appliances) that cannot fully disable split-tunneling while the tunnel is connected (as defined above) does not meet this security policy.

3) VPNs may be client-based or LAN-to-LAN-based.

a. Client-based VPNs are VPNs in which a software (client) is installed on a remote user's computer and a secure connection is made between that VPN client and a VPN-capable terminating device. (i.e. VPN concentrator, firewall, router, server).

b. LAN-to-LAN VPNs are VPNs that are created between a VPN-capable device on a third party network and a VPN-capable device on the State network.

4) In implementing VPNs, tunnels should be limited with access-restrictions that are granular enough to restrict traffic to both IP addresses and specific TCP/UDP ports. The list of addresses and ports allowed must be pared down to only what is necessary for the applications used by the remote users.

5) ITS maintains Cisco VPN termination devices to establish client-based and LAN-to-LAN VPNs for access to resources on the State Network.

a. Direct telnet access via TN3270 from the Internet to the State Data Center is not permitted because Telnet sessions can be hijacked and the username/password are transmitted in clear text.

b. All LAN-to-LAN VPNs will be implemented using the IPSec protocol.

c. Any third party entity that needs a connection to the State Network must provide and maintain compatible industry-standard IPSec-capable VPN hardware/software solution at their end of the connection. VPN must be addressed using public IP addresses registered to that entity, including the peer address and any networks behind the third party VPN device that will be encrypted by the tunnel. The ITS side of the connection will adhere to the same rules, but with addresses provided by ITS.

d. Client-based VPNs may be implemented with IPSec or SSL.

6) At no time may an agency permit a third party entity to connect directly to their local area network behind the State's border firewall and/or the agency's firewall. This backdoor direct connection is a serious security violation. This includes terminating third party circuits behind ITS and agency firewalls and/or utilizing a PC remote control product (ie. PCAnywhere) and a modem over a dialup connection.

7) If an agency provides dial-in access to agency personnel either via a remote access service or PC modem on their LAN or via an outsourced remote access service, the Agency must implement a firewall to control access to and from the local area network by the dial users. The Agency will be held responsible for any dial user that uses their facilities to access and manipulate or abuse any other facility.

8) Based upon industry best practices and recommendations by leading industry security experts, ITS reserves the right to modify this policy for remote access and VPNs (ie. centralizing VPN services), as necessary, to be more productive and effective for the State.

XVII. Passwords; Guidelines, Protection of, Bad examples

Passwords are our personal identification keys that allow access to various IT resources on the State network. Passwords help ensure that only authorized individuals access a computer system, a network device, an application, a file, data, etc. Passwords also help to establish accountability for all transactions and changes made to those IT resources. Each State agency is responsible for enacting strict password policies in securing their segment of the State network infrastructure. ITS recommends that each State agency consider the following guidelines when developing these password policies.

Choosing a Password:

- Passwords must contain at least 8 nonblank characters.
- Passwords must contain a combination of letters (preferably a mixture of upper and lowercase letters), numbers, and at least one special character within the first seven positions. Examples of special characters include #, $, _, #, $, and @.
- Passwords may not contain the user ID.
- Passwords may not include the personal information about the user that can be easily guessed: user name, spouse's name, kids name, employee number, social security number, birth date, telephone number, city, etc.
- Passwords may not include common words from an English dictionary or foreign-language dictionary. Hackers have tools that can break any password found in a dictionary or that is a simple transformation of a dictionary word.
- Passwords may not contain commonly used proper names, including the name of any fictional character or place.
- Passwords may not contain any simple pattern of letters or numbers such as "qwertyxx" or "xyz123xx."

- Passwords should not be trivial, predictable or obvious.
- A complex password that cannot be broken is useless if you cannot remember it and have to write it down. For security to function, you must choose a password you can remember and yet is complex. For example, Msi5!YOld (My Son is 5 years old) OR IhliCf5#yN (I have lived in California for 5 years now).
- In addition, it is important to tailor your password to your system.
    - Some UNIX systems will only use the first eight characters of a password.
    - Oracle applications such as LETS only allow $, _, and # as special characters
    - UNIX passwords are case sensitive, so "password" is not the same as "PASSWORD". On the other hand, VMS passwords are not case sensitive, so "password" and "PASSWORD" are the same

- Examples of Bad Passwords:

alec7	Based on the user's name, too short, no special character, number cannot be at the end of a password.
Gillian	Girlfriend's name (also proper name), too short, no special character.
Naillig	Still a proper name, even though it's only backwards, too short, no special character.
PORSCHE911	Proper name, in the dictionary, no special character.
12345678	Number series, no special character, and people can easily watch as you type it.
Computer#	Still a dictionary word, even though it is capitalized, special character must be one of the first 7 characters.
wombat6	Dictionary word, no special character, number cannot be at end of password.
merde3	In a French dictionary; too short; number cannot be at end of password, no special character.
mr.spock	Name of a character, in a sci-fi dictionary.
zeo$lite	In a geological dictionary.
ze0$lite	Corrupted version of a word in a geological dictionary, easily deciphered

Protecting Passwords:

- Do not disclose your passwords to anyone except in emergency circumstances or when there is an overriding operational necessity (i.e., support issue). If you are required to give your password to someone (even agency support staff), change the password as soon as they are through.
- Do not leave passwords in a location accessible to others or secured in a location for which protection is less than that required for information that the password protects.
- Passwords should never be written down.
- Use Secure Shell (SSH) to avoid sending your password in clear text over the network. Crackers can break into a network, set up a program called a sniffer that listens to the network for passwords, and steal your password. Anytime you type your password to log in to another computer using telnet, ftp, rlogin, etc., your password can be stolen.
- Passwords should be unique to users and users should never share passwords.
- Passwords should be changed at least every 6 months and never reused.
- Never use default passwords. All passwords should be unique. This is especially important for administrator accounts with extended rights..
- Passwords should be required on all user accounts.
- Don't let support vendors have free reign of agency IT resources. If a vendor needs access to some resource for support, give the vendor a password and then change it and lock them out when their support is complete.
- Be diligent about removing user accounts for staff no longer employed by agency.
- Users should log out when leaving their desk for extended periods of time. Especially administrative users with extended rights.
- If you suspect your password has been stolen or "cracked", change it immediately.

XVIII. Servers; Operating Systems, Security and Version Control

Because of their service role, it is common for servers to store many of an organization's most valuable and confidential information resources. They also are often deployed to provide a centralized capability for an entire organization, such as communication/email or user authentication. Security breaches on a network server can result in the disclosure of critical information or the loss of a capability that can affect the entire organization. Therefore, securing network servers should be a significant part of your network and information security strategy.

Many security problems can be avoided if servers and networks are appropriately configured. Default hardware and software configurations, however, are set by vendors who tend to emphasize features and functions more than security. Since vendors are not aware of your security needs, you must configure new servers to reflect your security requirements and reconfigure them as your requirements change.

There are several aspects of network servers that can make them tempting targets for hackers/intruders:

- Public servers often have publicly known host names and IP (Internet Protocol) addresses.
- Public servers may be deployed outside an organization's firewall or other perimeter defenses.
- Servers usually actively listen for requests for services on known ports, and they try to process such requests.
- Servers often do not have a human user who notices signs of unusual activity.
- Servers are often remotely administered, so they willingly accept connections from privileged accounts.
- Servers often are configured to reboot automatically after some kinds of failures, which can offer opportunities for intruders.

The following recommendations are designed to help you configure and deploy network servers that satisfy your organization's IT needs, as well as, your security requirements. These recommendations are generic in nature and should be considered for all servers including: Novell, Windows NT, UNIX, Linux, Windows XP, etc. Please consider these recommendations when deploying servers in the network:

1) Do not purchase or deploy systems that fail to meet your security requirements.

2) As a general rule, a network server should be dedicated to a single service. This usually simplifies configuration, which reduces the likelihood of configuration errors. It also can eliminate unexpected and unsafe interactions among the services that present opportunities for intruders.

3) Determine what steps you need to take to ensure that the information contained on hardware being replaced, removed from service, or disposed of is eliminated to the extent possible. For example, erase and reformat disks, rewrite tapes, and clear firmware passwords from servers being taken out of commission. Hackers could use information gathered from old hard drives, to crack other systems.

4) Prevent the use of a network server as a workstation.

5) Stay informed of vendors' security-related updates to their products, which may be called updates, upgrades, patches, service packs, or hot fixes. Whenever an update is released, you need to evaluate it, determine if it is applicable to your organization's computers, and, if so, install it. The most common sources of current information include Web sites of vendors and computer- and network-security organizations. There are also mailing lists, some of which are sponsored by vendors, and USENET news groups. KEEP SECURITY PATCHES CURRENT.

6) Offer only essential network services and operating system services on the server host machine. Other services can be used to attack the host and impair or remove desired network services. Either do not install unnecessary services or turn the services off and remove the corresponding files (and any other unnecessary files) from the host.

7) Remove unneeded default accounts and groups. The default configuration of the operating system often includes guest accounts, administrator accounts, and accounts associated with local and network services. The names and passwords for those accounts are well known. Remove or disable unnecessary accounts to eliminate their use by intruders.

8) Change default passwords. For default accounts that you want to keep on the system, change the passwords to make it harder for intruders to compromise the accounts. Also disable passwords for accounts that need to exist but do not require an interactive login.

9) Ensure users follow your password policy. Document your password policy, communicate it to users, and train them to always follow the policy. Configure the password-setting software to reject passwords that don't conform to your policy, if the operating system provides this feature.

10) Configure servers to deny login after a small number of failed attempts. It is relatively easy for an unauthorized user to gain access to a server by using automated software tools that attempt all passwords. If your operating system provides the capability, configure it to deny login after three failed attempts. Typically, the account is "locked out" for a period of time (such as 30 minutes) or until a user with appropriate authority reactivates it.

11) Configure computer operating systems with appropriate object, device, and file access controls. Many operating systems provide the capability to specify access privileges individually for files, devices, and other data or code objects. We recommend that you configure the settings on files and other objects to take advantage of this capability and protect information stored on the computer. By carefully setting access controls, you can reduce both intentional and unintentional security breaches. For example, denying read access helps to protect confidentiality of information, and denying unnecessary write access can help maintain the integrity of information. Limiting the execution privilege of most system-related tools to authorized system administrators can prevent most users from making configuration changes that could reduce security. It also can restrict the ability of intruders to use those tools to attack the system or other systems on the network. Only give users access to files/data that they need.

12) Identify and implement server logging mechanisms. For example, access to services should be logged and/or protected through access-control methods such as TCP Wrappers, etc.

13) Develop and implement a file backup and restoration plan. File backups allow you to restore the availability and integrity of information resources following security breaches and accidents. Without a backup, you may be unable to restore a computer's data after system failures and security breaches.

14) Install virus scanning software and aggressively scan for viruses. Also, keep virus definition files up-to-date. Scanning for viruses with out-dated antivirus software will not detect the "latest and greatest" virus threats traveling around the Internet.

15) Deploy servers in a secure facility preventing unauthorized access to the server.

16) Deploy network wiring and devices in a secure facility. For example, if an intruder gains access to a network switch, he can place a "sniffer" on the network and "sniff" for data including sensitive/personal data, passwords etc.

17) Implement appropriate change management procedures and all configuration changes to server must follow those procedures.

18) Never log into a server and use root/supervisor/administrator access when a non-privileged account login will work.

XIX. Security Tools; Scanners and Intrusion Detection Systems

An Intrusion Detection System (IDS) monitors computer systems and network traffic and analyzes that data for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the enterprise. The main advantage of an IDS is that it provides a view of server and network activity and issues alerts notifying administrators of unauthorized, unusual activity. While IDS can identify that an intrusion has occurred or is in process, and it may be able to provide the intruder's IP address, the security administrator or network manager must then investigate the attack, determine how it occurred, and correct the problem. Human intervention is also required to recognize false alarms and override possible system lock out for those occasions.

ITS has implemented IDS devices on the State network in strategic locations to actively and aggressively monitor the State IT core infrastructure for intrusion attempts. These strategic locations help ITS monitor intrusion attempts from outside the State "trusted" network and as well as, attacks from within the State "trusted" network. When an IDS identifies an action that appears to be an intrusion attempt, the IDS sends commands to the appropriate core device (i.e. switch, router and/or firewall) to block any traffic from the offending IP address.

ITS is in the process of implementing a security monitoring and management framework that will enable us to capture and correlate information from the existing network devices and to provide detailed reporting in a interactive, real-time environment. This security monitoring and management framework will enable ITS to capture large volumes of data from the existing network devices (IDS, firewalls, routers, host systems, authentication servers, etc.), correlate and present it in a useful reporting format to help ITS technical staff in detecting, identifying and stopping unauthorized IT infrastructure access.

With the existing IDS devices and soon-to-be implemented security monitoring framework, ITS will be monitoring the State core infrastructure for intrusion detection attempts. It is recommended that each Agency purchase IDS devices to specifically monitor their segment of the State network, including firewalls, routers, switches, host systems, etc. These Agency-specific IDS devices would send data back to the ITS security monitoring and management framework so that the agency's ITS resources could be monitored for intrusion detection and corrective action taken on a 24/7 basis. If an agency is interested in implementing this type of technology, they should contact the ITS Security Officer for details.

Also, ITS believes we should practice "defense in depth". If we assume that major network firewall and servers can be compromised (which they can by patient and skilled hackers), then unprotected client/desktop systems behind these compromised firewalls can be usurped and used as internal launching points for attacks on the agency/state network. Statistics have shown the majority of attacks come from within. Personal firewall capability on each of the client/desktop systems can significantly reduce this inside threat. Therefore, because of the threat from the "inside", ITS recommends that each agency consider an additional level of security by implementing personal firewall software on each client/desktop system on their network.

XX. Physical Access; Security Guidelines and Recommendations

A majority of security violations, vandalism, and even accidental acts that lead to disruption of services can be attributed to deficiencies in physical security. The guidelines below should be considered in order to maintain adequate physical security for each agency.

Location

(1) Locate computer equipment in inconspicuous places without signs, maps, and external references.

(2) Locate equipment away from windows or any other place that allows easy access by outside individuals.

(3) Locate computer installations in places that can be environmentally controlled.

(4) Insure that computer installations are located away from heavy traffic patterns.

(5) Insure that all equipment, even PCs, can be located in rooms that can be physically secured.

(6) Locate equipment in areas to minimize the likelihood of accidents. For example, do not place equipment in rooms that contain overhead water pipes or in rooms next to large mechanical systems.

(7) Try to locate facilities in buildings that are of less risk as far as disaster potential. Buildings located in flood zones, near railroad tracks, or remote to fire departments would be at greater risk.

Access Control

(1) Larger computer installations must be equipped with an access control system, normally a card access system. Access then can be limited to specific individuals at specific times and dates. Dates and times can be recorded to track access. Specific procedures must be in place to control the assignment and authorization level of access to facilities and to terminate access should access requirements change. Other than the access control system, larger installations should:

- Require security related clearance as a result of employment. (For example, all ITS employees that have access to State Data Center facilities are sworn in as Information Confidentiality Officers as defined by legislation and are subject to background checks).
- Use cameras to record activity in and around computer installation.
- Archive access system and video data for a period of one year.
- Restrict visitors in the computer facilities. Visitors must sign in and must be accompanied by an authorized staff member.

(2) Smaller computer installations, especially those that contain critical servers, must be kept in locked rooms. The number of individuals with access to the room must be limited.

(3) Any PC that is connected to an agency LAN or to the state Wide Area Network must be placed in a room that can be locked after hours. Any PC that is left unattended during the day should be disconnected from the network when left or placed in rooms that can be locked.

(4) Any PC that contains critical information should be located in a room that can be locked.

(5) Wiring closets should be locked at all times.

(6) Rooms or closets that contain State Wide Area Network routers or switches must be locked at all times. This includes remote offices.

(7) Agencies should insure that all laptops are stored in secure locations and that there is a strict checkout procedure for issuing laptops to staff members.

Environmental and Electrical Measures

(1) Computer facilities must have fire protection. Larger facilities should have a pre-action fire suppression system installed. All facilities must have strategically placed hand held fire extinguishers. Fire extinguishers must be inspected yearly by the Fire Department.

(2) All facilities must deploy smoke and heat detectors.

(3) Flammable or toxic materials must not be stored near computer equipment.

(4) Larger installations must deploy water detectors.

(5) Electrical systems for critical computer equipment must include Uninterrupted Power Systems (UPS). A generator should be considered for this critical equipment also. Surge protectors should be considered for equipment sensitive to power fluctuations.

(6) Larger facilities must insure that adequate room temperature and humidity is maintained to the specifications of the hardware vendor. Redundancy must be built into any HVAC system. Any system should include facilities for monitoring the environment and sounding alarms should threshold exceed norms.

(7) Areas housing environmental or electrical systems critical to computer facilities should be protected by access control systems and monitored by security cameras.

Miscellaneous Physical Security Measures

(1) Each agency should locate alternate space that meets the same physical security requirements for a business recovery site.

(2) Backup and recovery materials (tapes, manuals, etc.) must be kept at a site that meets stringent physical security measures.

XXI. Non-State-Business Related Network Traffic

Bandwidth has a high cost associated with its usage. The State network was implemented and is maintained to allow State employees to utilize automated systems and tools to help facilitate their carrying out work responsibilities and duties and meeting the needs of those individuals they serve. In saying that, the State network infrastructure must not be utilized for personal gain and/or entertainment. Unnecessary applications that pose potential security risks will not be permitted on the State network. These include, but are not limited to:

1) AOL/Yahoo Instant Messaging protocols outbound from State network to Internet will not be permitted.

2) Music/video/file sharing services (I.e. Napster, Kazaa, etc.) will not be permitted on State network. In addition to security concerns, these services are bandwidth "monsters". Single users of these systems have the potential to consume the majority of an Agency's bandwidth potential.

3) No streaming audio/video from Internet to State network will be permitted. These applications sometimes trigger false positives within the intrusion detection sensor. In addition to security concerns, these services also consume large amounts of bandwidth network-wide.

ITS also has an Acceptable Use Policy in place and recommends that each agency enact an acceptable use policy for their own computer infrastructure. The ITS Acceptable Use Policy is provided as Exhibit A to this document.

XXII. Wireless Networking

The purpose of this policy is to outline security and data integrity measures required for implementing and securing wireless local area networks that reside within the State of Mississippi's wide area network. Agencies must understand that unsecured wireless networks are a serious breach of security. Any unauthorized and/or neglectful installations of wireless networks that expose the State's network infrastructure to intruders and/or attacks may result in that agency's connection to the State network being isolated. Also, any agency that implements a wireless network solution assumes all responsibility and will be held accountable for all unauthorized State network intrusions, loss of data/systems, and hack attacks attributed to their wireless network.

An agency should not undertake wireless deployment for any operations until it has examined and can acceptably manage and mitigate the risks to its information, system operations, and continuity of essential operations. Maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems. Therefore, it is important that agencies assess risks more frequently and test and evaluate system security controls when wireless technologies are deployed.

Before implementing a wireless network, agencies must notify Telecommunication Services of their intent to do so. If the agency has already implemented a wireless solution, agencies must notify Telecommunication Services of the existing deployment. At this time, ITS recommends the use of wireless network technology only as a solution for special or unique business requirements and not for general-purpose deployment.

At minimum, the following security standards and network configurations are **required** for the deployment and operation of all wireless network installations:

1) The placement of wireless LAN Access Points (WAP) must be strategically located to prevent the interception of wireless signals by unauthorized individuals or outside the intended coverage area. WAPs should be mounted above ceiling tiles, out of plain site, or otherwise publicly inaccessible and not visible to unauthorized persons. The range of WAPs must also be tested to ensure that signals are not being transmitted outside the intended coverage area.

2) All WAP installations must use the strongest native standard of encryption available for the device. At minimum, WPA Version 1 with (128bit) TKIP as the encryption mechanism is required. However, it is recommended that WPA Version 2, also known as 802.11i with (256 bit) AES as the encryption mechanism be utilized for the highest level of security. WEP is easily broken and, therefore, not permitted.

3) Both WPA Version 1 and 2 may be deployed in either "PSK mode" or "Enterprise mode" with specific requirements for each mode.

a. PSK mode deployment requirements

i. The "key" or "pass-phrase" should be known and kept securely by as few personnel as possible.

ii. The "key" or "pass-phrase" should be changed regularly. Regularly is defined as every six months for minimum standards, however, it is recommended to be changed every three months.

iii. Very strong password creation practices should be followed when creating WPA-PSK passwords. At minimum, 16 characters with alpha-numeric, upper case, lower case and special characters should be used. Do not use words easily found in a dictionary or common phrases.

iv. This mode can be used to minimize network overhead

v. May be used when remote clients are not mobile and the network administrator can easily control and change the passwords regularly.

b. Enterprise mode deployment requirements

i. Recommended as most secure method for protecting wireless data.

ii. This option requires the use of an 802.1x client supplicant software and a Radius server.

4) WPA Version 1 and 2 PSK Mode is the minimum requirement for fixed, wireless bridges. Must meet the criteria detailed in 3.a.

5) All WAP configuration parameters (Service Set Identifier (SSID), keys, passwords, channels, etc) that can be changed from the default manufacturer settings must be changed from the default. Also, the beacon interval on the WAP must be set to the longest interval possible. Where applicable, the new settings should be complex and not easily discerned or provide clues to the location, agency, or data / system description.

6) WAP connections must be restricted to only identified, expected, listed, and known Message Authentication Code (MAC) addresses.

7) WAPs must be connected to a LAN switch and not a LAN hub. An ethernet hub will transmit data to every node on the network, including the wireless LAN segment. An intruder will not only be able to see data transmitted over the wireless LAN but also from the LAN.

8) Physical security of WAPs must be maintained to protect the WAP from theft or access to the data port.

9) The SSID should not openly identify the LAN or it's purpose, and should be constructed as securely as a password. Open broadcasting of the SSID must be disabled.

10) Agencies should consider the use of VPNSs for specific users or network segments that need to transmit sensitive and confidential information or data for an added measure of security on top of WPA protocols.

11) Software and firmware updates from the wireless manufacturer should be applied to the WAP and affected wireless cards as soon as possible after release to keep the security updated.

Additionally, the following wireless security best practices are recommended for deployment and operation of a wireless network.

1) All WAP installations should be inventoried and the area in which the wireless LAN is installed must be regularly inspected for unauthorized WAPs or other devices not part of the approved installation. The network should be regularly inspected both physically, and electronically using sniffing tools to uncover rogue WAPs and devices.

2) Dynamic Host Configuration Protocol (DHCP) on wireless networks is strongly discouraged. DHCP can provide automatic IP network identification to any wireless device, including an intruder.

3) WAP configuration settings should be periodically assessed to ensure security mechanisms are being properly implemented. There are various tools on the market that can be used for capturing WAP configurations.

4) Periodic security reviews should be conducted to ensure that changes to the wireless LAN have not exposed the network to intruders. In addition, the network should be periodically scanned to detect unauthorized devices.

XXIII. Emergency Response Team

Each agency should designate an individual as the liaison between the agency and the ITS Emergency Response Team that addresses security violations or intrusions. This designee will be considered part of the State Emergency Response Team, will receive pertinent security related information, and will attend regular meetings to discuss security issues within the State infrastructure. An ITS Emergency Response Team will be composed of the Data Services Director, the Data Network Manager, the Data Center Security Administrator, the Network Security Officer, and the Strategic Services' Security Coordinator.

The ITS Emergency Response Team will be responsible for following a strict set of procedures to collect information associated with a violation or intrusion, report the incidence to the proper authorities, and ultimately perform actions within the security infrastructure to remedy the situation. The ITS Emergency Response Team is also responsible for disseminating information to the agencies concerning procedures for reporting incidences.

XXIV. Security Incident Procedures, Reporting, Preserving Evidence, Legal Action

State agencies, through the Emergency Response Team liaison, must report all violations or suspected violations to the ITS Emergency Response Team. ITS will then work with the agency to ensure evidence is preserved and that it is reported correctly. The ITS Emergency Response Team, working with the agency liaison, will then:

- Respond quickly to ensure that traces, logs, etc. are intact and available. Processing will not be stopped immediately. No files will be restored immediately.
- Communicate via the telephone. Some intruders may be able to monitor E-mail.
- Make copies of files that the intruder may have altered of left.
- Make sure the perpetrator is not directly contacted.
- Identify a primary contact to handle evidence.
- Contact the FBI and local Law Enforcement.

It is the responsibility of all State employees and/or contractors to report suspected security violations as quickly as possible. Subsequent action, depending on the type of breach, can vary. Security breaches may be categorized as those pertaining to physical intrusions, electronic intrusions that include networks, servers, and workstations; incidents related to catastrophic disasters, and breaches as a result of deception and/or fraud. The ultimate goal, regardless of the category of incident, is the protection of state assets, containment of damage, and the restoration of service.

Security Incident Reporting – All types of security breaches

1. Keep a Log

Logging of pertinent information is critical in situations which may eventually involve criminal prosecution. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a **written** log should be kept for security incidents that are under investigation. The Security Incident Reporting form (under development) should be used to document the incident details.

2. Notification of Incident

Informing the appropriate people is of extreme importance. All employees and/or contractors should immediately report any suspected security breach to their manager or agency director. The Security Incident Reporting form should be used to document the incident details. Managers or agency directors should notify the Chief Information Confidentiality Officer (Director of the Mississippi Department of Information Technology) immediately.

3. Release of Information

Control of information during the course of a security incident or investigation of a possible incident is very important. All releases of information should be authorized by the Chief Information Confidentiality Officer of ITS or the Board of the Mississippi Department of Information Technology Services.

4. Follow up Analysis

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow up analysis should be performed. All involved parties should meet and discuss the actions that were taken and the lessons learned. All existing procedures should be evaluated and modified.

Additional requirements pertaining to specific categories of security violations

- For a physical intrusion of secured areas, notification may also include the Department of Finance and Administration Law Enforcement, the Mississippi Highway Patrol and/or local police department.
- For catastrophic disasters such as fire, bomb threats, floods, or destructive storms, notification procedures should include the local fire department and/or police department.
- For incidents involving electronic intrusions, other state agencies should be notified as appropriate. Any data captured that resulted in detecting the intrusion should be kept until the incident has been investigated and cleared.
- For incidents involving deception and fraud, additional notification may include the police department depending upon the severity of the incident.

Electronic Data Security Violations

System Implementation and Administration Procedures

- Normal logging processes should be enabled on all host and server systems.
- Alarm and alert functions, as well as logging, of any firewalls and other network perimeter access control systems should be enabled.
- System integrity checks of the firewalls and other network perimeter access control systems should be performed on a routine basis.
- Audit logs from the perimeter access control systems should be reviewed daily.
- Audit logs for servers and hosts on the internal, protected network should be reviewed on a weekly basis.
- Users should be trained to report any anomalies in system performance to their system administration staff, as well as relevant network or information systems security staff.
- All trouble reports received by system administration personnel should be reviewed for symptoms that might indicate intrusive activity. Suspicious symptoms should be reported to Network or Information Systems security personnel.

Types of Hacker Incidents

1. Attempts to Gain Access to a System

Incidents of this type may include repeated login attempts, repeated "ftp" or "telnet" commands, and repeated dial back attempts.

Identify the problem – Identify the source of attack by looking at system log files and active network connections. Make copies of all audit trail information such as system log files, the root history file, utmp and wtmp files, etc. **LOG ALL ACTIONS**.

Notification – The incident should be reported following the procedures outlined in Security Incident Reporting procedures. A follow up report should also be completed.

2. Active Hacker/Cracker Activity

There are two methods for dealing with an active hacker/cracker incident.

The first method is to immediately lock the person out of the system and restore the system to a safe state.

The second method is to allow the hacker/cracker to continue his probe/attack and attempt to gather information that will lead to an identification and possible criminal conviction. The method used to handle a cracker/hacker incident should be determined by the level of understanding of the risks involved.

In the case of an active hacker/cracker activity, a decision should be made whether to allow the activity to continue while evidence is gathered or to get the hacker/cracker off the system and then lock the person out. The Director of the Mississippi Department of Information Technology Services, or designee, or ITS Executive level management should make this decision. The decision should be based on the availability of qualified personnel to monitor and observe the hacker/cracker and the level of risk involved.

3. Evidence of Past Hacker/Cracker Incidents

When an incident is discovered after the fact, there is not always a lot of evidence available to identify the person or how they gained access to the system. If you should discover that someone had successfully broke into a system, the incident should be reported following the procedures outlined in the Security Incident Reporting policy.

Removal of Hacker/Cracker

Snap-shot of the system – Make copies of all audit trail information such as system log files, the root history files, etc. Also get a listing of all active network connections. **LOG ALL ACTIONS**.

Lock Out the Hacker – Kill all active process for the hacker/cracker and remove any files or programs that he/she may have left on the system. Change passwords for any accounts that were accessed by the hacker/cracker. **LOG ALL ACTIONS**.

Restore the System – Restore the system to a normal stage. Restore any data or files that the hacker/cracker may have modified. Install patches or fixes to close any security vulnerabilities that the hacker/cracker may have exploited. All actions taken to restore the system to a normal state should be documented in a logbook. **LOG ALL ACTIONS**.

Report the Incident – The incident should be reported following the procedures outlined in the Security Incident Reporting policy.

Follow up – After the investigation, a short report describing the incident and actions that were taken should be documented and distributed to the appropriate personnel.

Monitoring of Hacker/Cracker Activity

There are no set procedures for monitoring the activity of a hacker. However, monitoring information should be recorded in a written log. Each incident should be dealt with on a case by case basis. The person authorizing the monitoring activity should provide direction to those doing the monitoring. Once the decision has been made to cease monitoring the hacker's activities and have him removed from the system, the steps outlined previously (Removal of Hacker/Cracker) should be followed.

State of Mississippi
Department of Information Technology Services
Information Technology Security Incident Report

Report Date/Time: _____

SECTION 1
Point of Contact (POC) Information

Name: _____

Title: _____

Telephone/Fax Number: _____

E-mail: _____

Organization: _____

Address: Street: _____

City: _____

State: _____

Zip Code: _____

Country: _____

SECTION 2

Incident Information

1. Name of Organization: (if same as above, enter "SAME")

   Organization's contact Information:

   Telephone Number:

   Address: (if same as above, enter "SAME")

   Street:

   City, State, Zip Code:

   Country:

   E-mail:

2. Physical location (s) of victim's computer system/network (Be Specific):

3. Date/Time and duration of incident:

4. Is the affected system/network critical to the organization's mission?

☑ Yes ☐ No

5.

☐ Intrusion	☐ System impairment/denial resources
☐ Unauthorized root access	☐ Web site defacement
☐ Compromise of system integrity	☐ Hoax
☐ Theft	☐ Damage
☐ Unknown	☐ Other:

6. Has this problem been experienced before? (If yes, please explain in the remarks section):

☐ Yes ☑ No

Remarks: No Remarks

7. Suspected method of intrusion/attack (check only **one**)

- ☐ Virus (provide name if known)
- ☐ Denial of Service
- ☐ Distributed Denial of Service
- ☐ Unknown
- ☐ Vulnerability exploited (explain)
- ☐ Trojan horse
- ☐ Trapdoor
- ☐ Other (Provide details in remarks)

8.

Remarks: No Remarks

9. Suspected perpetrator(s) or possible motivation(s) of the attack (check only **one**)

- ☐ Insider/Disgruntled employee
- ☐ Competitor
- ☐ Unknown
- ☐ Former employee
- ☐ Other (Explain in remarks)

Remarks: No Remarks

10. The apparent source (IP address) of the intrusion/attack:

11. Evidence of spoofing?

- ☐ Yes
- ☐ No
- ☐ Unknown

12. What computer system (hardware and/or software) was affected? (Operating system, version) (check only **one**):

- ☐ Unix
- ☐ Linux
- ☐ NT
- ☐ Sun OS/Solaris
- ☐ OS2
- ☐ VAX/VMS
- ☐ Windows
- ☐ Other (Provide specify in remarks)

Remarks: No Remarks

13. What security infrastructure was in place? (Check all that apply)

- ☐ Incident/Emergency Response Team
- ☐ Firewall
- ☐ Intrusion Detection System
- ☐ Security Auditing Tools
- ☐ Packet filtering
- ☐ Encryption
- ☐ Secure Remote Access/Authorization tools
- ☐ Banners
- ☐ Access Control Lists

14. Did the intrusion/attack result in a loss/compromise of sensitive, classified or proprietary information?

☐ Yes (Provide details in remarks) ☐ No

☑ Unknown

Remarks: No Remarks

15. Did the intrusion/attack result in damage to system(s) or data?

☐ Yes (Provide details in remarks) ☑ No

Remarks: No Remarks

16. What actions and/or technical mitigation have been taken?

- ☐ System(s) disconnected from the network
- ☐ System Binaries checked
- ☐ Backup of affected system(s)
- ☐ Other (Please provide details in remarks)
- ☐ Log files examined
- ☐ No action(s)

Remarks: No Remarks

17. Has the local FBI field office been informed?

☐ Yes (Which Office) _____ ☒ No

18. Has another agency/organization been informed? If so, please provide name and phone number.

☐ Yes ☒ No

- State/local police: _____
- Inspector General: _____
- CERT-CC _____
- FedCIRC _____
- JTF-CNO _____
- Other (Incident Response, law enforcement,etc.) _____

19. When was the last time your system was modified or updated?

Date:

Company/Organization that did the work (address, phone number, POC information):

20. Is the System Administrator a contractor?

☐ Yes (Provide POC Information) ☒ No

21. In addition to being used for law enforcement or national security purposes, the intrusion-related information I reported may be shared with:

☐ Other State/Federal Agencies ☐ The Public

22. Additional Remarks: (Please limit to 500 characters. Amplifying information may be submitted separately.)

No additional remarks

SECTION 3

ITS Contact Information

If the reported incident is determined to be a criminal matter you may be contacted by an agent in your location for additional information.

Email completed form to: Steven Walker at walker@its.state.ms.us
Snail Mail to Steven Walker: 301 North Lamar Street, Suite 508, Jackson, MS 39201
Phone ITS Network Operations Center: 601-359-1405

Exhibit B

POLICY STATEMENT REGARDING APPROPRIATE, ACCEPTABLE USE OF INFORMATION TECHNOLOGY FACILITIES AND RESOURCES OF MISSISSIPPI DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES

The following is ITS's formal policy statement regarding appropriate, acceptable use of information technology facilities and resources of Mississippi Department of Information Technology Services. The Mississippi Department of Information Technology Services (ITS) is dedicated to providing the best possible service to its customers and is committed to ensuring that the information systems resources of the State and ITS are used appropriately for the purposes they are intended.

This policy governs the use of all computers, computer-based communications networks, and all related equipment administered by ITS. A user is defined as any person employed by ITS, which includes full-time, part-time, temporary, contract employees, persons who are employed by contractors or subcontractors of ITS, and any other individuals who are authorized to use agency information systems. The electronic communications and facilities of ITS are the property of the State and **by using these facilities the user acknowledges consent to abide by this policy**. These facilities and resources are to be used for state business purposes. The user should be aware that any communications or use of the ITS information systems resources are not to be considered private or confidential, and can be monitored at any time. All users are hereby notified that system security features allow any messages or usage to be monitored and archived regardless of passwords and message deletions, and that computer use is subject to search and monitoring at any time. Access can be traced back to the individual.

For any questions, ask your supervisor or the ITS Personnel Director for clarification or additional information. For any related issue not specifically addressed here, please ask your supervisor or the ITS Personnel Director.

Software:

1) Software, including but not limited to Internet downloads, utilities, add-ins, programs (including shareware, freeware and Internet access software), patches, upgrades, or clip-art, shall not be installed on any desktop, notebook personal computer (PC), or server by anyone other than a representative of the Internal Data Processing (IDP) unit of ITS, without notification to IDP via e-mail or Help Me ticket. There are to be no games on any desktop, PC, or server at any time for any reason. All software purchased for use on ITS equipment must be approved in writing by IDP. The agency's network contains software which performs an inventory of each PC on a regular basis to ensure compliance with this rule.

2) Software owned or licensed by ITS may not be copied to alternate media, distributed by e-mail, transmitted electronically, or used in its original form on other than ITS PCs without express written permission from IDP. In no case is the license agreement or copyright to be violated.

3) Standard software is to be used for all internal functions. Approved non-standard software is only to be used to interface with customer or vendor organizations when they require the non-standard software.

4) Software licensed to ITS is to be used for its intended purpose according to the license agreement. Employees are responsible for using software in a manner consistent with the licensing agreements of the manufacturer. License agreements are maintained by IDP.

Hardware:

1) All PCs, workstations, printers, add-in cards, memory modules, and other associated equipment are the property of the State of Mississippi and should not be used for purposes other than business. No changes, modifications, additions, or equipment removals may be done without notification to IDP via e-mail or Help Me ticket.

2) Except notebook PCs used in daily offsite work, no information systems equipment should be removed from ITS premises without the permission of your supervisor. In the event equipment is to be off premises for some time, the employee responsible for the equipment must file a written hand receipt with the ITS Property Officer.

Practices:

1) No materials are to be disseminated in any manner which are derogatory to any person or group, obscene, racist, sexist, harassing or offensive based on color, religion, creed, national origin, age or disability.

2) System identification codes and passwords are for the use of the specifically assigned user and are to be protected from abuse and/or use by unauthorized individuals.

3) All diskettes, e-mail attachments and executable e-mail messages are automatically scanned for viruses using the virus detection software installed on all ITS computer workstations which have been configured by IDP. If you have made any configuration changes to your workstation, even with the approval of IDP, it is your responsibility to ensure virus protection prior to opening/executing diskettes, e-mail attachments or executable e-mail messages.

4) Like all ITS information systems resources, Internet access and e-mail are for work-related use. Access and sites visited can and will be monitored at the specific individual level.

5) Employees may not use ITS information systems resources for soliciting, personal financial gain, partisan political activities or further disseminating "junk" e-mail such as chain letters.

6) Information contained on the agency network and workstations is strictly proprietary to the State of Mississippi and ITS. Copying or disseminating any of this information for any purpose other than state business is strictly prohibited. Access to this information must be considered confidential.

7) You are expected to report violations of this policy which you observe to your supervisor or, in the event that the violation involves the supervisor, the ITS Personnel Director. Likewise, if you are a witness to a violation you are required to cooperate in any investigation of the violation.

Consequences:

Any user who knowingly and willingly violates this policy is subject to discipline up to and including termination from employment depending on the severity of the specific offense(s). Furthermore, in the event of an illegal activity, the user will also be reported to the appropriate law enforcement authority.

If you have any question regarding this policy or any situation not specifically addressed in this policy, see your supervisor or the ITS Personnel Director.

Revision:

This policy is subject to revision. ITS will adequately post revisions, but it is the user's responsibility to ensure that use of the ITS computing and communication resources conforms to current policy.

Appendix 1

Organization Structure & Contact Info

Name	Title	Phone	Email
Roger Graves	Telecommunications Services (TS) Director	601-359-2892	roger.graves@its.state.ms.us
Jimmy Webster	Telecommunications Services (TS) Assistant Director	601-359-2690	jimmy.webster@its.state.ms.us
Steven Walker	Project Manager	601-359-2624	steven.walker@its.state.ms.us
Greg Nohra	TS Engineer	601-359-5209	greg.nohra@its.state.ms.us

Glossary

D

DMZ

A computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

DNS

An Internet service that translates *domain names* into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name *www.example.com* might translate to *198.105.232.4*.

E

E-commerce

Business that is conducted over the Internet using any of the applications that rely on the Internet, such as e-mail, instant messaging, shopping carts, Web services, UDDI, FTP, and EDI, among others. Electronic commerce can be between two businesses transmitting funds, goods, services and/or data or between a business and a customer.

F

FTP

The protocol for exchanging files over the Internet. FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies, FTP uses the Internet's TCP/IP protocols to enable data transfer.

H

HTTP

The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

I

ICMP

An extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

IMAP

A protocol for retrieving e-mail messages. The latest version, *IMAP4*, is similar to *POP3* but supports some additional features. For example, with IMAP4, you can search through your e-mail messages for keywords while the messages are still on mail server. You can then choose which messages to download to your machine.

IPSec

A set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs).

N

NAT (Network Address Translation)

An Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A *NAT box* located where the LAN meets the Internet makes all necessary IP address translations.

P

POP

A protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an *e-mail client*) use the POP protocol, although some can use the newer IMAP (Internet Message Access Protocol).

S

SMTP

A protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.

Split Tunneling

The process of allowing a remote VPN user to access a public network, most commonly the Internet, at the same time that the user is allowed to access resources on the VPN. This method of network access enables the user to access remote devices, such as a networked printer, at the same time as accessing the public network.

SSH

A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSL

A protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers.By convention, URLs that require an SSL connection start with *https:* instead of *http*:.

W

Web Server

A computer that delivers (*serves up*) Web pages. Every Web server has an IP address and possibly a domain name. For example, if you enter the URL *http://www.pcwebopedia.com/index.html* in your browser, this sends a request to the server whose domain name is *pcwebopedia.com*. The server then fetches the page named *index.html* and sends it to your browser.